Finite Fields and Their Applications 16 (2010) 401–405

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

An estimate on the number of stable quadratic polynomials

Domingo Gomez *, Alejandro P. Nicolás *

Departamento de Matemáticas, Estadística y Computación, Universidad de Cantabria, Santander, Spain

ARTICLE INFO

Article history:
Received 22 January 2010
Revised 28 June 2010
Available online 22 July 2010
Communicated by D. Panario

MSC:
11T06
37C75
37C20

Keywords:
Irreducible polynomials
Composition of polynomials
Stable quadratic polynomials

ABSTRACT

In this work we obtain a nontrivial estimate for the size of the set of triples $(a,b,c) \in \mathbb{F}_q^* \times \mathbb{F}_q \times \mathbb{F}_q$ which correspond to stable quadratic polynomials $f(X) = aX^2 + bX + c$ over the finite field $\mathbb{F}_q$ with q odd. This estimate is an improvement of the bound $O(q^{11/4})$ conjectured in a recent work of A. Ostafe and I. Shparlinski.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of q elements with q odd. For a polynomial $f(X) \in \mathbb{F}_q[X]$ we define the following sequence:

$$f^{(0)}(X) = X, \qquad f^{(n)}(X) = f^{(n-1)}\big(f(X)\big), \quad n \geqslant 1.$$

We say that $f \in \mathbb{F}_q[X]$ is *stable* if $f^{(n)}$ is irreducible over $\mathbb{F}_q$ for all $n \geqslant 0$. In the following, we only work with polynomials of degree 2, that is,

$$f(X) = aX^2 + bX + c \in \mathbb{F}_q[X], \quad \text{with } a \neq 0.$$

Our aim is to study the number of triples $(a,b,c) \in \mathbb{F}_q^* \times \mathbb{F}_q \times \mathbb{F}_q$ which corresponds to these stable polynomials. According to [1], we denote this number as S_q. This problem is related with the size of

* Corresponding authors.
E-mail addresses: domingo.gomez@unican.es (D. Gomez), alejandro.p.nicolas@unican.es (A.P. Nicolás).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2010.06.005

multiplicative character sums. Let us denote by $\gamma = -b/(2a)$ the critical point of f, that is, the zero of the derivative f'. The *adjusted orbit of* f is defined as:

$$Orb(f) = \left\{ f^{(n)}(\gamma) \,\middle|\, n > 1 \right\} \cup \left\{ -f(\gamma) \right\}.$$

It can be proved (see [2] and [3]) that a quadratic polynomial f over $\mathbb{F}_q$ is stable if and only if $Orb(f)$ contains no squares.

The cardinality of the subset of squares in a set can be estimated by means of character sums. In particular, it can be done using the only nontrivial quadratic multiplicative character χ of $\mathbb{F}_q$. The *Weil bound* for character sums will be useful to estimate the bounds of S_q and can be presented in the following form (see Chapter 5 of [4]).

Lemma 1. *Let χ be the multiplicative quadratic character of $\mathbb{F}_q$ and let $F(X) \in \mathbb{F}_q[X]$ be a polynomial of positive degree that is not, up to a multiplicative constant, a square polynomial. Let d be the number of distinct roots in its splitting field over $\mathbb{F}_q$. Under these conditions, the following inequality holds*

$$\left| \sum_{x \in \mathbb{F}_q} \chi\left(F(x)\right) \right| \leqslant (d-1) q^{1/2}.$$

2. Estimate of S_q

This section is devoted to find an estimate of the bounds for S_q. Our main result is the following one.

Theorem 1. *For any q odd, if S_q is the number of stable quadratic polynomials $f \in \mathbb{F}_q[X]$, then*

1. $S_q \geqslant (q-1)^2/4$,
2. $S_q = O(q^{5/2} \log q)$.

The next result will be useful for calculating the lower and upper bounds of the number of stable quadratic polynomials.

Lemma 2. *For any stable polynomial $f(X)$ and $a \in \mathbb{F}_q^*$,*

$$g_a(X) = \frac{f(aX)}{a} \in \mathbb{F}_q[X]$$

is a stable polynomial. Moreover, the number of stable polynomials is a multiple of $q-1$.

Proof. Given a stable polynomial $f(X)$, let us consider the map

$$\begin{aligned} \varphi : \mathbb{F}_q^* &\longrightarrow \mathbb{F}_q[x], \\ a &\longrightarrow g_a. \end{aligned}$$

It is easy to see that $g_a^{(n)}(X) = a^{-1} f^{(n)}(aX)$ for all $n \geqslant 0$. So, if $h(X) \mid g_a^{(n)}(X)$, then $h(a^{-1}X) \mid f^{(n)}(X)$ and g_a is stable for all $a \in \mathbb{F}_q^*$. Moreover, the map φ is always injective provided that f is stable. In such case, since $f = a_0 X^n + \cdots + a_d$ is irreducible, $a_d \neq 0$. So, $g_a = g_b$ if and only if $a = b$. Henceforth, the number of stable polynomials is a multiple of $q-1$. □

Now, using Proposition 3 of [5], we will establish the lower bound. We can distinguish two different cases:

1. If $q \equiv 1 \pmod 4$, then the adjusted orbit of the polynomial of $\mathbb{F}_q[x]$ given by $f_b(X) = (X-b)^2 + b$ is $Orb(f_b) = \{b, -b\}$. This orbit does not contain any squares provided that b is not a square of $\mathbb{F}_q^*$. Since there exist $(q-1)/2$ elements such that are not squares in $\mathbb{F}_q^*$, we have, at least, $(q-1)/2$ of such stable quadratic polynomials.
2. If $q \equiv -1 \pmod 4$ and $u, v \in \mathbb{F}_q$ are such that $u^2 + v^2 = -1$, the adjusted orbit of the polynomial $f_u(X) = (X - 4u^2 - 2)^2 + 4u^2$ is $Orb(f_u) = \{-4u^2, -4v^2\}$, which does not contain any squares of $\mathbb{F}_q$. From Lemma 6.24 of [4], we know that there exist $q+1$ solutions of the equation $u^2 + v^2 = -1$ in $\mathbb{F}_q^2$. Since $f_u = f_v$ if and only if $u^2 = v^2$, there are at least $(q+1)/4$ of such stable quadratic polynomials.

Finally, Lemma 2 with the bounds obtained for $q \equiv 1 \pmod 4$ and $q \equiv -1 \pmod 4$ leads us to the first statement of Theorem 1.

In what follows, we will establish the upper bound of Theorem 1. Using the previous notation, we define $F_{(k)}(a, b, c) = f^{(k)}(\gamma)$, where a, b, c are variables and $\gamma = -b/(2a)$. From [1], we have that

$$S_q \leqslant \frac{1}{2^K} \sum_{a \in \mathbb{F}_q^*} \sum_{b,c \in \mathbb{F}_q} \prod_{k=1}^{K} \big(1 - \chi\big(F_{(k)}(a,b,c)\big)\big), \quad \forall K \in \mathbb{Z}^+. \tag{1}$$

Expanding the products and rearranging the terms, we conclude that there are $2^K - 1$ sums of the shape

$$(-1)^{\mu} \sum_{(a,b,c) \in \mathbb{F}_q^* \times \mathbb{F}_q \times \mathbb{F}_q} \chi\left(\prod_{j=1}^{\mu} F_{(k_j)}(a,b,c) \right), \quad 1 \leqslant k_1 < \cdots < k_\mu \leqslant K,$$

with $\mu \geqslant 1$ and one trivial sum corresponding to 1 in (1). This sum can be transformed in

$$\begin{aligned} &\sum_{(a,b,c) \in \mathbb{F}_q^* \times \mathbb{F}_q \times \mathbb{F}_q} \chi\left(\prod_{j=1}^{\mu} F_{(k_j)}(a,b,c) \right) \\ &\quad = \sum_{(a,b,c) \in \mathbb{F}_q^* \times \mathbb{F}_q \times \mathbb{F}_q} \chi\left(\prod_{j=1}^{\mu} F_{(k_j)}\big(a,b,c - b/2 + b^2/4\big) \right). \end{aligned} \tag{2}$$

From Lemma 2, it suffices to consider $a = 1$; so $F_{(k_j)}(1, b, c - b/2 + b^2/4)$ is monic. The upper bound will be obtained multiplying by $q-1$. The following result will be used in the deduction of the upper bound.

Lemma 3. *For fixed integers $k_1, \ldots, k_\mu$ such that $1 \leqslant k_1 < \cdots < k_\mu \leqslant K$, the polynomial*

$$\prod_{j=1}^{\mu} F_{(k_j)}\big(1, Y, c - Y/2 + Y^2/4\big)$$

has a multiple root only for at most $2^K(K-2) + 2$ choices of c.

Proof. First of all, we will see that, for all $n \geqslant 0$, the function $F_{(n)}(1, Y, c - Y/2 + Y^2/4)$ is linear in Y and has degree 2^{n-1} in c.

Let us consider the polynomial $f(X) = X^2 + YX + (c - Y/2 + Y^2/4)$. Then, $\gamma = -Y/2$ and $F_{(0)}(1, Y, c - Y/2 + Y^2/4) = f(\gamma) = c - Y/2$. Also,

$$f\big(f(\gamma)\big) = (c - Y/2)^2 + Y(c - Y/2) + \big(c - Y/2 + Y^2/4\big).$$

So, $F_{(1)}(1, Y, c - Y/2 + Y^2/4) = c^2 + c - Y/2 = g^{(0)}(c) - Y/2$, with $g^{(0)} = Z^2 + c$. Let us now suppose that this formula is valid for n; therefore

$$\begin{aligned} f^{(n+1)}(\gamma) = f\big(f^{(n)}(\gamma)\big) &= \big(g^{(n-1)}(c) - Y/2\big)^2 + Y\big(g^{(n-1)}(c) - Y/2\big) \\ &\quad + \big(c - Y/2 + Y^2/4\big) = \big(\big(g^{(n-1)}(c)\big)^2 + c\big) - Y/2 = g^{(n)} - Y/2, \end{aligned}$$

which proves that $F_{(n)}(1, Y, c - Y/2 + Y^2/4) = g^{(n-1)}(c) - Y/2$ for all n. Notice that, as we have claimed, this polynomial is linear in Y and has degree 2^{n-1} in c.

Given $1 \leqslant k_1 < \cdots < k_\mu \leqslant K$, the polynomial $\prod_{j=1}^{\mu} F_{(k_j)}(1, Y, c - Y/2 + Y^2/4)$ has a multiple root if and only if some of the numbers $g^{(k_j-1)}(c)$ are equal. That is, if and only if c is a root of some of the polynomials

$$g_{t,s}(Z) = g^{(t)}(Z) - g^{(s)}(Z), \quad 0 \leqslant s < t \leqslant K - 1.$$

So, the number of multiple roots of the polynomial $\prod_{j=1}^{\mu} F_{(k_j)}(1, Y, c - Y/2 + Y^2/4)$ is bounded by the number of roots of the polynomials $g_{t,s}(Z)$ for $0 \leqslant s < t \leqslant K - 1$. Since each of these polynomials has at most 2^t roots for all $0 \leqslant s \leqslant t - 1$, the total number of multiple roots is bounded by $\sum_{t=1}^{K-1} t2^t = 2^K(K - 2) + 2$. □

We are now able to establish the upper bound of Theorem 1. The trivial sum of (1) can be bounded by $O(q^3/2^K)$. For the other terms, we can use the Weil bound, given in Lemma 1, for those polynomials which are not squares. Since these polynomials have at most degree K (see the proof of Lemma 3), we obtain $O(Kq^{5/2})$ for this part. For the rest, that is, the polynomials with at least one multiple root, we can use a trivial bound. Thus, from Lemma 3, we get $O(2^K Kq^2)$. Then,

$$S_q = O\big(q^3/2^K + Kq^{5/2} + 2^K Kq^2\big).$$

Choosing $2^K = O(q^{1/2})$, we obtain $S_q = O(q^{5/2} \log q)$. Theorem 1 is proved.

3. Final remarks and comments

The main achievement of this work was the establishment of upper and lower bounds for the number of stable quadratic polynomials over a finite field $\mathbb{F}_q$. The lower bound has been set using the work of Ali (see [5]), which guarantees the existence of such polynomials for any q odd. For the upper bound, in order to relate the number of stable quadratic polynomials with the sum of the quadratic character of $\mathbb{F}_q$, we have used the ideas presented in [1]. In both cases, the results were derived from Lemma 2, which holds for stable polynomials of any degree. Furthermore, it is also true for fields of characteristic zero, as can be seen in Lemma 6 of [6].

Acknowledgments

D.G. was partially supported by the Spanish Ministry of Science, project MTM2007-67088. The authors want to thank Alina Ostafe and Igor Shparlinski for comments and helpful advice. Also, many thanks to Arne Winterhof, who found a slot in his schedule to read the paper.

Finally, the authors thank the referee for many useful comments and suggestions that certainly contributed to the improvement of the paper.

References

[1] A. Ostafe, I. Shparlinski, On the length of critical orbits of stable quadratic polynomials, Proc. Amer. Math. Soc. 138 (8) (2010) 2653–2656.
[2] R. Jones, N. Boston, Settled polynomials over finite fields, Preprint.
[3] M. Ayad, D.L. McQuillan, Irreducibility of the iterates of a quadratic polynomial over a field, Acta Arith. 93 (1) (2000) 87–97.
[4] R. Lidl, H. Niederreiter, Finite Fields and Applications, Cambridge, 1997.
[5] N. Ali, Stalilité des polynômes, Acta Arith. 119 (2005) 53–63.
[6] O. Ahmadi, F. Luca, A. Ostafe, I. Shparlinski, On stable quadratic polynomials, Preprint.